§ 9.2 Implementation and oversight responsibilities.

The Order requires each agency that originates or handles classified information to promulgate implementing regulations. The Order further requires that each agency originating or handling classified material shall designate a senior official to direct and administer its information security program. This official shall be responsible for actively overseeing the agency's program, including a security education program, to ensure effective implementation of the Order.

(a) In addition, this official shall have the following responsibilities:

(1) To establish and monitor agency policies and procedures to prevent over or under classification, to ensure the protection from unauthorized disclosure of properly classified information, including intelligence information, and to ensure orderly and effective declassification of agency documents which no longer require protection, in accordance with the terms of the Order.

(2) To review proposed classified disclosures of an exceptional nature bearing upon issues of concern to the Congress and the public.

(3) To issue any needed guidelines for classification or declassification.

(4) To recommend to the agency head the following:

(i) Proposals for reclassification in accordance with section 1.6(c) of the Order;

(ii) Other categories of information, as defined in section 1.3(a)(10) of the Order, which require protection against unauthorized disclosure but which are not specifically protected by sections 1.3(a) (1) through (9) of the Order;

(iii) Waivers, for specified classes of documents or information of the requirement to indicate which portions of documents are classified and which are not, as provided by section 1.5(b) of the Order; and

(iv) Waivers for specified classes of documents or information, of the requirement to prepare derivative classification guides, as provided by section 2.2(c) of the Order.

(5) To prepare a list of officials, by name or position, delegated Top Secret, Secret, and Confidential classification authority.

(6) To receive, and if necessary act on, suggestions and complaints with respect to that agency's administration of its information security program.

(7) To provide guidance concerning corrective or disciplinary action in unusually important cases involving unauthorized disclosure or refusal to declassify.

(8) To maintain liaison with the Director of ISOO and to furnish reports and information as required by section 5.2 of the Order.

(b) *Department of State.* Within the Department of State, the senior official is the Deputy Assistant Secretary, Classification/Declassification Center, hereinafter referred to as (DAS/CDC).

(c) *AID.* Within AID (a component of the International Development Cooperation Agency), the senior official is the Inspector General.

(d) *USIA.* Within USIA, the senior official is the Director, Office of the Public Liaison.

§ 9.3 Responsibility for safeguarding classified information.

(a) *Primary.* The specific responsibility for the maintenance of the security of classified information rests with each person having knowledge or physical custody thereof, no matter how obtained.

(b) *Individual.* Each employee is responsible for becoming familiar with and adhering to all security regulations.

(c) *Supervisory.* The ultimate responsibility for safeguarding classified information rests upon each supervisor to the same degree that the supervisor is charged with functional responsibility for the organizational unit. While certain employees may be assigned specific security responsibilities, such as Top Secret Control Officer or Unit Security Officer, it is nevertheless the basic responsibility of supervisors to ensure that classified material entrusted to their organizational units is handled in accordance with the procedures prescribed in these regulations. Each supervisor should ensure that no one employee is assigned unreasonable security responsibilities in addition to usual administrative or functional duties.

(d) *Organizational.* The Offices of Security in State, AID, and USIA are responsible for physical, procedural, and personnel security in their respective agencies. In the Department of State, the Office of Communications (COMSEC) is responsible for communications security.

§9.4 Classification.

(a) When there is reasonable doubt about the need to classify information, the information shall be safeguarded as if it were "Confidential" pending a determination about its classification by an original classification authority. When there is reasonable doubt about the appropriate classification level, the information shall be safeguarded at the higher level pending the determination of its classification level by an original classification authority. Determinations hereunder shall be made within 30 days.

(b) Information may not be classified unless its disclosure reasonably could be expected to cause damage to the national security. Information may not be classified to conceal violations of law, inefficiency, or administrative error; to prevent embarrassment to a person, organization, or agency; to restrain competition; or to prevent or delay the release of information that does not require protection in the interest of national security.

(c) The President or an agency head or official designated under section 1.2 (a)(2), 1.2 (b)(1), or 1.2 (c)(1) of the Order may reclassify information previously declassified and disclosed if it is determined in writing that (1) the information requires protection in the interest of national security, and (2) the information may reasonably be recovered. These reclassification actions shall be reported promptly to the Director of ISOO.

(d) It is permitted to classify or reclassify information after an agency has received a request for it under the Freedom of Information Act or the Privacy Act, or the mandatory review provisions of the Order, provided that such classification meets the requirements of the Order and is accomplished personally and on a document-by-document basis by the agency head, the deputy agency head, the senior official, or an official with original Top Secret classification authority. Every effort should be made to classify properly at the time of origin. When a determination is made that a document requires classification or reclassification, however, all holders of the document should be notified and, in the Department of State, a copy of the classification or reclassification memorandum should be sent to the Foreign Affairs Information Management Center (FAIM). In addition, if the classification or reclassification was done in any office other than the DAS/CDC, that office should send a copy of the pertinent memorandum to the CDC.

(e) For the Department of State, these functions will be performed by the DAS/CDC.

(f) For AID, the function will be performed by the Administrator.

(g) For USIA, the function will be performed by the Director of Public Liaison.

(h) Information classified in accordance with these regulations shall not be declassified automatically as a result of any unofficial publication or inadvertent or unauthorized disclosure in the United States or abroad of identical or similar information.

§9.5 Classification designations.

(a) Only three (3) designations of classification are authorized: "Top Secret," "Secret," and "Confidential."

(1) *Top Secret.* Information may be classified "Top Secret" if its unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security. This classification should be used with the utmost restraint. Examples of "exceptionally grave damage" include armed hostilities against the United States or its allies; disruption of foreign relations vitally affecting the national security; the compromise of vital national defense plans or complex cryptologic and communications intelligence systems; the revelation of sensitive intelligence operations; and the disclosure of scientific or technological developments vital to national security.

(2) *Secret.* Information may be classified "Secret" if its unauthorized disclosure could reasonably be expected to